AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) In a computing system having one or more input devices and a storage medium, a method of ~~operation~~ enciphering data comprising:

receiving through the one or more input devices a first permutation specification of a first permutation of a first plurality of data inputs;

receiving through the one or more input devices a first permutation modifier;

receiving through the one or more input devices an interaction specification of a first interaction between the first permutation and the first permutation modifier; ~~and~~

automatically generating and storing in the storage medium a second permutation specification of a second permutation of the first plurality of data inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier;

generating a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification; and

activating said cryptography engine to apply said second permutation specification to a set of data to encipher said set of data.

2. (Original) The method of claim 1 wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

3. (Currently Amended) The method of claim 1 wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of data inputs.

4. (Original) The method of claim 3 wherein the third permutation specification specifies the third permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

5. (Currently Amended) The method of claim 3 wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the data inputs to the third permutation.

6. (Original) The method of claim 3 wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

7. (Original) The method of claim 1 wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

8. (Original) The method of claim 1 wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

9. (Original) The method of claim 1 wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first permutation are moved to be outputs immediately to the left of those specified in the first interaction specification.

10. (Original) The method of claim 1 wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

11. (Original) The method of claim 1 wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

12. (Original) The method of claim 1 wherein the first and second permutations comprise 32 bit permutations.

13. (Cancelled).

14. (Currently Amended) The method of claim ~~13~~ 1 further comprising configuring the programmable cryptography engine based at least in part on the generated configuration vector.

15. (Currently Amended) The method of claim 1 further comprising:

receiving through the one or more input devices a second permutation modifier;

receiving through the one or more input devices a second interaction specification of a second interaction between the second permutation and the second permutation modifier;

automatically generating and storing in the storage medium a third permutation specification of a third permutation of the first plurality of data inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier;

generating another configuration vector to configure the programmable cryptography engine based at least in part on the third permutation specification; and

activating said cryptography engine to apply said third permutation specification to another set of data to encipher said another set of data.

16. (Cancelled).

17. (Currently Amended) A computer readable medium comprising:

a storage medium; and

a plurality of executable instructions stored in the storage medium, and designed to program a computing device having one or more input devices and memory to enable the computing device to:

receive through the one or more input devices a first permutation specification of a first permutation of a first plurality of data inputs;

receive through the one or more input devices a first permutation modifier;

receive through the one or more input devices an interaction specification of a first interaction between the first permutation and the first permutation modifier; ~~and~~

automatically generate and store in the memory a second permutation specification of a second permutation of the first plurality of data inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier;

generate a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification; and

activate said cryptography engine to apply said second permutation specification to a set of data to encipher said set of data.

18. (Original) The computer readable medium of claim 17 wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

19. (Currently Amended) The computer readable medium of claim 17 wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of data inputs.

20. (Currently Amended) The computer readable medium of claim 19 wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the data inputs to the third permutation.

21. (Original) The computer readable medium of claim 19 wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

22. (Original) The computer readable medium of claim 17 wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

23. (Original) The computer readable medium of claim 17 wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

24. (Original) The computer readable medium of claim 17 wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first permutation are moved to be outputs immediately to the left of those specified in the first interaction specification.

25. (Original) The computer readable medium of claim 17 wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

26. (Original) The computer readable medium of claim 17 wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

27. (Cancelled).

28. (Currently Amended) The computer readable medium of claim ~~27~~17, wherein the executable instructions are further designed to enable the computing device to configure the programmable cryptography engine based at least in part on the generated configuration vector.

29. (Currently Amended) The computer readable medium of claim 17, wherein the executable instructions are further designed to enable the computing device to:

receive through the one or more input devices a second permutation modifier;

receive through the one or more input devices a second interaction specification of a second interaction between the second permutation and the second permutation modifier;

automatically generate and store in a storage medium a third permutation specification of a third permutation of the first plurality of data inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier;

generate another configuration vector to configure the programmable cryptography engine based at least in part on the third permutation specification; and

activate said cryptography engine to apply said third permutation specification to another set of data to encipher said another set of data.

30. (Cancelled).

31. (Currently Amended) A computing device comprising:

one or more input devices;

a storage medium having stored therein a first plurality of executable instructions designed to enable the computing device to:

receive through the one or more input devices a first permutation specification of a first permutation of a first plurality of data inputs;

receive through the one or more input devices a first permutation modifier;

receive through the one or more input devices an interaction specification of a first interaction between the first permutation and the first permutation modifier; and

automatically generate and store in the storage medium a second permutation specification of a second permutation of the first plurality of data inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier; ~~and~~

generate a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification; and

activate said cryptography engine to apply said second permutation specification to a set of data to encipher said set of data; and

at least one processor coupled to the storage medium to execute the instructions.

32. (Previously Presented) The computing device of claim 31, wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

33. (Currently Amended) The computing device of claim 31, wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of data inputs.

34. (Currently Amended) The computing device of claim 33, wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the data inputs to the third permutation.

35. (Previously Presented) The computing device of claim 33, wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

36. (Previously Presented) The computing device of claim 31, wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

37. (Previously Presented) The computing device of claim 31, wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

38. (Previously Presented) The computing device of claim 31, wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first permutation are moved to be outputs immediately to the left of those specified in the first interaction specification.

39. (Previously Presented) The computing device of claim 31, wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

40. (Previously Presented) The computing device of claim 31, wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

41. (Cancelled).

42. (Currently Amended) The computing device of claim 4131, wherein the executable instructions are further designed to configure the programmable cryptography engine based at least in part on the generated configuration vector.

43. (Currently Amended) The computing device of claim 31, wherein the executable instructions are designed to:

receive through the one or more input devices a second permutation modifier;

receive through the one or more input devices a second interaction specification of a second interaction between the second permutation and the second permutation modifier; and

automatically generate and store in the storage medium a third permutation specification of a third permutation of the first plurality of data inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier;

generate another configuration vector to configure the programmable cryptography engine based at least in part on the third permutation specification; and

activate said cryptography engine to apply said third permutation specification to another set of data to encipher said another set of data.

44. (Cancelled).